

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-231486  
(43)Date of publication of application : 22.08.2000

(51)Int.Cl. G06F 9/06  
G06F 12/14

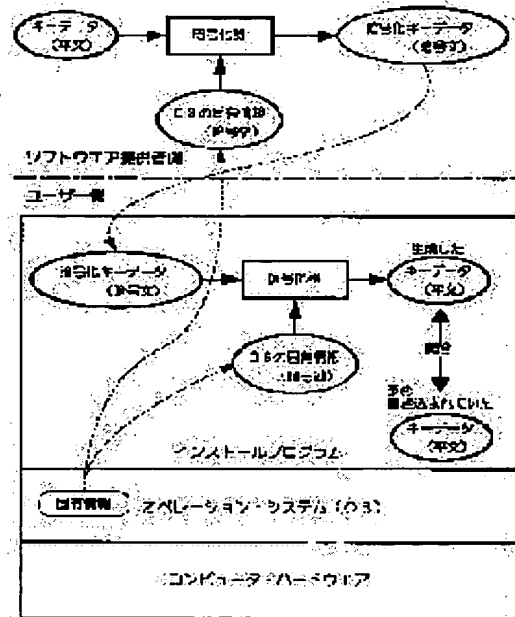
(21)Application number : 11-031141 (71)Applicant : TOYO COMMUN EQUIP CO LTD  
(22)Date of filing : 09.02.1999 (72)Inventor : TANAKA HIROYUKI

## (54) METHOD FOR PREVENTING SOFTWARE FROM ILLEGALLY BEING COPIED

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To enable illegal copying prevention which uses key data enabling installation in only the computer of a user by obtaining the key data by deciphering inputted ciphered key data with characteristics information of the computer and carrying on the installation of software only when the key data are true.

**SOLUTION:** An installation program functions as a decipherer and generates the key data by deciphering the ciphered key data by using version information read by an operation system as a key. The installation program compares the generated key data with key data written in a program in advance to decide whether or not the key data are true and continues to install the software main body only when the key data generated in response to the coincidence between the both are true. Then the generated key data are compared with the key data which are already written in the program and when the both do not match each other, it is decided that the key data are false, thereby quitting subsequent installing operation.



## LEGAL STATUS

[Date of request for examination]  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2000-231486  
(P2000-231486A)

(43)公開日 平成12年8月22日(2000.8.22)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 9/06	5 5 0	G 0 6 F 9/06	5 5 0 J 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 E 5 B 0 7 6

審査請求 未請求 請求項の数2 O L (全 5 頁)

(21)出願番号 特願平11-31141

(22)出願日 平成11年2月9日(1999.2.9)

(71)出願人 000003104

東洋通信機株式会社

神奈川県高座郡寒川町小谷2丁目1番1号

(72)発明者 田中 弘之

神奈川県高座郡寒川町小谷二丁目1番1号

東洋通信機株式会社内

Fターム(参考) 5B017 AA07 BA07 CA15

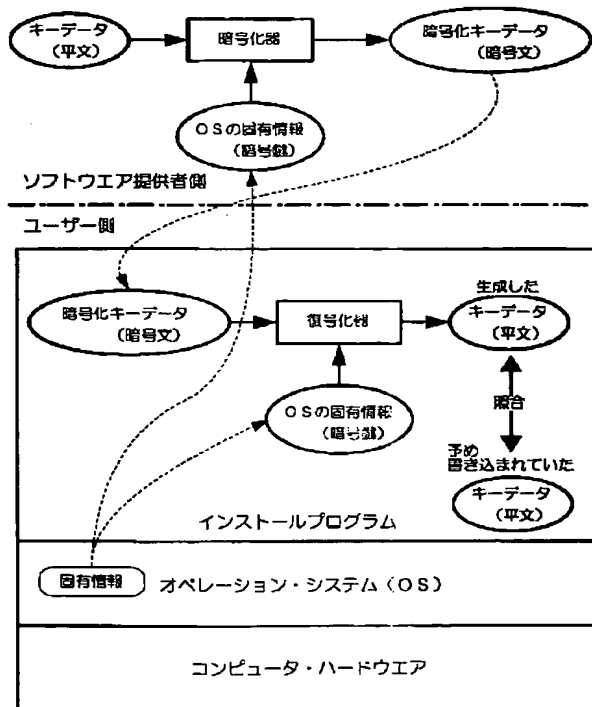
5B076 FA05

(54)【発明の名称】 ソフトウェアの不正コピー防止方法

(57)【要約】

【課題】 C D - R O M等の読み出し専用の記録媒体によるソフトウェアの提供であっても、ユーザーのコンピュータのみにインストール可能とする不正コピー防止方法を提供する。

【解決手段】 オペレーティングシステムに与えられた固有情報により暗号化した暗号化キーデータを生成し、ソフトウェアを前記オペレーティングシステム上にインストールする際に、前記暗号化キーデータを入力した時のみインストールを継続し完了可能とする。



**【特許請求の範囲】**

【請求項1】 ソフトウェアをコンピュータにインストールする際に所定のキーデータを入力することにより不正コピーを防止する方法であって、  
予め前記キーデータを前記コンピュータの固有情報により暗号化した暗号化キーデータを生成するステップと、  
前記ソフトウェアをインストールする際に前記暗号化キーデータの inputs を促すステップと、  
コンピュータの固有情報を取得するステップと、  
入力された暗号化キーデータを固有情報により復号化してキーデータを得るステップと、  
復号化したキーデータの真偽を認証するステップと、  
前記キーデータが真であった時のみソフトウェアのインストールを継続するステップとを有するソフトウェアの不正コピー防止方法。

【請求項2】 オペレーティングシステム上で動作するソフトウェアをコンピュータにインストールする際に所定のキーデータを入力することにより不正コピーを防止する方法であって、  
予め前記キーデータを前記オペレーティングシステムに与えられた固有情報により暗号化した暗号化キーデータを生成するステップと、  
前記ソフトウェアをインストールする際に前記暗号化キーデータの inputs を促すステップと、  
オペレーティングシステムから固有情報を取得するステップと、  
入力された暗号化キーデータを固有情報により復号化してキーデータを得るステップと、  
復号化したキーデータの真偽を認証するステップと、  
前記キーデータが真であった時のみソフトウェアのインストールを継続するステップとを有するソフトウェアの不正コピー防止方法。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】 本発明は、ソフトウェア提供者から提供されるCD-ROM等の記録媒体からソフトウェアをコンピュータにインストールする際の不正コピー防止方法に関するものである。

**【0002】**

【従来の技術】 ソフトウェアを記録媒体で提供するにあたっては、そのソフトウェアが複数のシステムに不正コピーされるのを防ぐ為に、不正コピー防止方法が提案されている。例えば、フロッピーディスク等の書き込み可能な記録媒体にプログラムを記録してユーザーに提供し、インストール実行時に所定のデータを記録媒体に書き加えることにより、この記録媒体を用いての次回以降のインストールを不可能としたり、インストール回数を制限する方法があった。

【0003】 しかし、この方法では正規のユーザーであっても種々のトラブルを解消する為に再インストールす

ることが出来ないと云う不具合を生ずる。また、近年ではソフトウェアの多機能化によりプログラムの容量が増大しつつあり、大容量記憶媒体としてCD-ROMを用いるのが一般的となっている。ところが読み出し専用のCD-ROMによるソフトウェアの提供では上記の方法は実施不可能であり、不正コピーを防止できないという不具合があった。

【0004】 そこで、例えば、インストールの実行時にインストールプログラムがキーデータの inputs をユーザーに促し、キーデータの inputs が無い場合はそれ以降のインストールが継続できない様にしたり、ソフトウェアの一部機能の使用を制限する方法が最も一般的となっている。

**【0005】**

【本発明が解決しようとする課題】 しかしながら、例えばそのキーデータが文字や数字であればユーザーがその内容を容易に理解することができることから、複数のコンピュータに同じキーデータを用いてソフトウェアをインストール可能であり、また、たとえそのキーデータが暗号化されたものであってもキーデータとしては単独のファイル等により取り扱われるために、キーデータ自体のコピーは容易となることから、ユーザーが一度キーデータを入手した後は不正コピーが可能であり、不正コピー防止が不完全となるという不具合があった。そこで、各コンピュータがネットワークにて接続されている場合は、同じネットワーク内では同じキーデータを用いてインストールしたソフトウェアが同時に起動しないようにすると云ったプロテクトも採用されているが、個人ユーザーやネットワークに繋がっていないスタンドアロンで運用されているコンピュータへの不正コピーを防止することは出来なかった。本発明は、上記問題点を解決すべくなされたものであって、CD-ROM等の読み出し専用の記録媒体によるソフトウェアの提供であっても、ユーザーのコンピュータのみにインストール可能なキーデータを用いた不正コピー防止方法を提供することを目的とする。

**【0006】**

【課題を解決するための手段】 上記目的を達成すべく本発明は、ソフトウェアをコンピュータにインストールする際に所定のキーデータを入力することにより不正コピーを防止する方法であって、予め前記キーデータを前記コンピュータの固有情報により暗号化した暗号化キーデータを生成するステップと、前記ソフトウェアをインストールする際に前記暗号化キーデータの inputs を促すステップと、コンピュータの固有情報を取得するステップと、入力された暗号化キーデータを固有情報により復号化してキーデータを得るステップと、復号化したキーデータの真偽を認証するステップと、前記キーデータが真であった時のみソフトウェアのインストールを継続するステップとを有するもの、もしくは、オペレーティング

システム上で動作するソフトウェアをコンピュータにインストールする際に所定のキーデータを入力することにより不正コピーを防止する方法であって、予め前記キーデータを前記オペレーティングシステムに与えられた固有情報により暗号化した暗号化キーデータを生成するステップと、前記ソフトウェアをインストールする際に前記暗号化キーデータの inputs を促すステップと、オペレーティングシステムから固有情報を取得するステップと、入力された暗号化キーデータを固有情報により復号化してキーデータを得るステップと、復号化したキーデータの真偽を認証するステップと、前記キーデータが真であった時のみソフトウェアのインストールを継続するステップとを有するものである。

【0007】

【発明の実施の形態】以下、本発明を実施例を示す図面に基づき詳細に説明する。図1は、本発明に係るソフトウェアの不正コピー防止方法の原理を説明する図であり、同図に於いて、一点鎖線より上側はソフトウェア提供者の、下側はユーザーのコンピュータシステムの動作を示すものである。まず、ユーザーはソフトウェアをインストールするコンピュータの固有情報をソフトウェア提供者に通知する。この固有情報としてはユーザーのコンピュータにインストールされているオペレーションシステムの固有情報を用いる。例えば、Microsoft社のウィンドウズに於いては「バージョン情報」と称される固有情報が付与されている。このバージョン情報は、「コントロールパネル」内の「システム」ファイルの情報タグに「09898-oem-003157-93844」の如き形式で書かれており、ソフトウェアを入手したユーザーはこれを読み取ってソフトウェア提供者に知らせればよい。そしてこのバージョン情報は、ウィンドウズをインストールする際に自動生成されるものであり、インストールする度に異なるものである。つまり、コンピュータ毎に固有情報が付与されていることになる。

【0008】ユーザーから固有情報を受け取ったソフトウェア提供者は、インストールに必要なキーデータを前記固有情報を暗号鍵として暗号化を行い、暗号化キーデータを生成する。そして、ソフトウェア提供者はこれをユーザーに送付する。

【0009】以下、インストールプログラムの動作を図2に示す機能フローチャートを併せて参照しながら説明する。ユーザーは、ソフトウェアのインストールをするべくインストールプログラムを起動する。（ステップ1）

インストールプログラムは、ユーザーに暗号化キーデータの inputs を促すべくコンピュータに接続されたモニターに暗号化キーデータの inputs 要求表示をする。（ステップ2）

ユーザーがソフトウェア提供者から受け取った暗号化キーデータをキーボードより入力すると（ステップ3）、

インストールプログラムはオペレーションシステムよりバージョン情報を読み取る。（ステップ4）

【0010】次に、インストールプログラムは復号化器として機能し、オペレーションシステムより読み取ったバージョン情報を鍵として前記暗号化キーデータを復号化してキーデータを生成する。（ステップ5）

そして、インストールプログラムは生成したキーデータと、予めプログラム中に書き込まれていたキーデータとを比較してその真偽を判定する。（ステップ6）

更に、両者が一致して生成したキーデータが真であったと認証された時のみソフトウェア本体のインストールを継続し完了する。（ステップ7）

【0011】一方、ステップ3に於いてユーザーが誤った暗号化キーデータをキーボードより入力すると、インストールプログラムはこの誤った暗号化キーデータをオペレーションシステムより読み取ったバージョン情報にて復号化してキーデータを生成する。すると、ステップ6に於いて、生成したキーデータと予めプログラム中に書き込まれていたキーデータとを比較しても両者が一致しないので、生成したキーデータを偽を判定してそれ以降のインストール作業を中断する。（ステップ8）

【0012】次に、インストールプログラムは生成したキーデータが偽と判断された回数を確認し（ステップ9）、所定回数以下であればユーザーに暗号化キーデータの再 inputs を促すべくコンピュータに接続されたモニターに暗号化キーデータの再 inputs 要求表示をする。（ステップ10）

正しい暗号化キーデータが inputs されるまでこれを繰り返し、生成したキーデータが偽と判断された回数が所定回数（この例では3回）以上になるとインストール作業を中止してインストールプログラムを終了することとなる。

【0013】以上説明したように、ユーザーがソフトウェアをインストールするコンピュータの固有情報をソフトウェア提供者に通知し、正規の暗号化キーデータを受け取らない限り当該ソフトウェアをコンピュータにインストールすることが出来ないものである。また、正規ユーザーであっても1つのソフトウェアを固有情報の異なる他のコンピュータに対してインストールすることは出来ない。つまり、ソフトウェア提供者はコンピュータの固有情報と暗号化キーデータの発行状況とを管理することにより容易に不正コピーを防止することが可能となる。このとき、コンピュータの固有情報とユーザーの個人情報（氏名・住所等）とを対にして管理することで、不正コピーを目的とした暗号化キーデータの発行要求を発見することが出来る。

【0014】更に、コンピュータは個々に異なる固有情報を有しており、正規ユーザーでない限りその固有情報に対応する暗号化キーデータをソフトウェア提供者から入手出来ない。ソフトウェア提供者が上記のように暗号

化キーデータの管理をしている以上、ソフトウェアを大量に不正コピーして販売する悪徳業者から不正コピーされたものを入手してもインストールすることは出来ず、こうした不正行為自体を未然に防止する上で極めて有効である。

【0015】なお、ソフトウェア提供者とユーザーとの間でデータのやりとりが必要となる為、ソフトウェアを購入してから暗号化キーデータを入手するまでの期間は、そのソフトウェアをユーザーが利用することが出来ないと云う問題もあるが、ソフトウェア提供者がインターネットのホームページを開設し、ユーザーがコンピュータの固有情報を送信すると自動的に暗号化キーデータを生成し、ユーザーに提供することによりタイムラグを大幅に短縮することが可能である。また、インターネットを利用できないユーザーのために1週間程度の動作期限付き暗号化キーデータをソフトウェアに同梱すると云った変形も可能であろう。尚、上記実施例に於いては、コンピュータの固有情報としてウインドウズのバージョン情報を用いているが本発明はこれのみに限定されるもので

はなく、コンピュータ固有の情報であればいかなる情報を用いても良いことはいうまでもない。

【0016】

【発明の効果】以上説明した如く本発明に係るソフトウェアの不正コピー防止方法は、CD-ROM等の読み出し専用の記録媒体によるソフトウェアの提供であっても、インストールを継続する為のキーデータを、コンピュータの固有情報にて暗号化し、ユーザーに提供するものであるから、固有情報の異なる他のコンピュータへの不正コピーを確実且つ容易に防止する上で著しい効果を奏する。

【図面の簡単な説明】

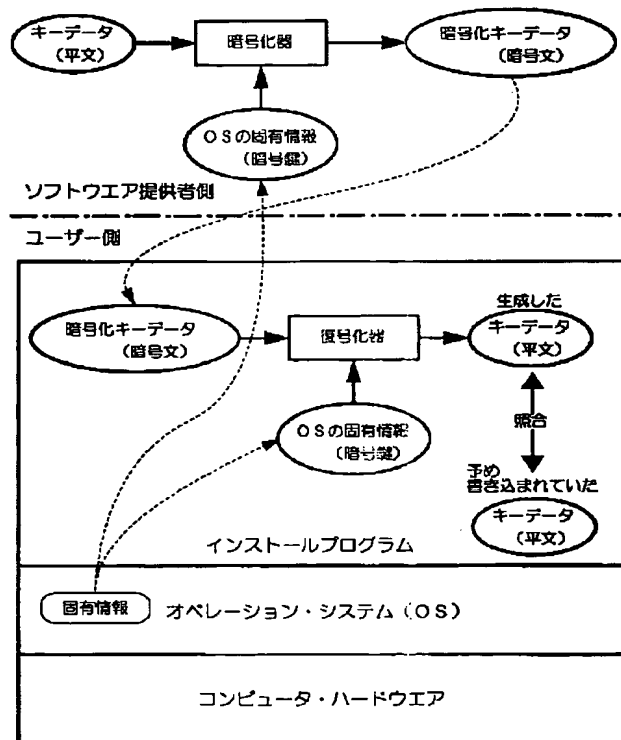
【図1】本発明に係るソフトウェアの不正コピー防止方法の原理を説明する図

【図2】本発明に係るインストールプログラムの動作を示す機能フローチャート

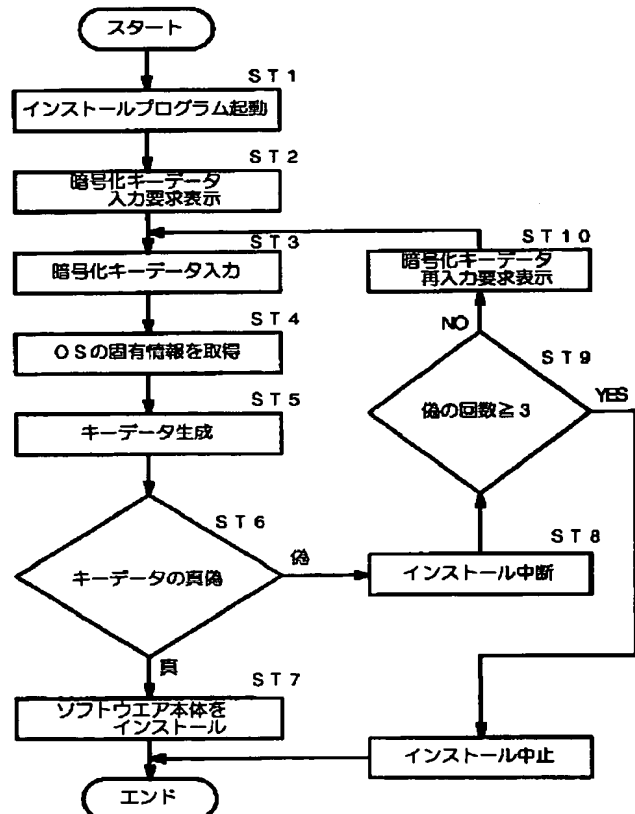
【符号の説明】

ST1～ST10 ……ステップ1?ステップ10

【図1】



【図2】



## 【手続補正書】

【提出日】平成11年2月9日(1999. 2. 9)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の詳細な説明

【補正方法】変更

【補正内容】

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ソフトウェア提供者から提供されるCD-ROM等の記録媒体からソフトウェアをコンピュータにインストールする際の不正コピー防止方法に関するものである。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】発明の詳細な説明

【補正方法】変更

【補正内容】

【発明の詳細な説明】

【0003】しかし、この方法では正規のユーザーであっても種々のトラブルを解消する為に再インストールすることが出来ないと云う不具合を生ずる。また、近年ではソフトウェアの多機能化によりプログラムの容量が増大しつつあり、大容量記憶媒体としてCD-ROMを用いるのが一般的となっている。ところが読み出し専用のCD-ROMによるソフトウェアの提供では上記の方法は実施不可能であり、不正コピーを防止できないという不具合があった。

## 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】発明の詳細な説明

【補正方法】変更

【補正内容】

【発明の詳細な説明】

【0005】

【本発明が解決しようとする課題】しかしながら、例えばそのキーデータが文字や数字であればユーザーがその内容を容易に理解することができることから、複数のコンピュータに同じキーデータを用いてソフトウェアをインストール可能であり、また、たとえそのキーデータが暗号化されたものであってもキーデータとしては単独の

ファイル等により取り扱われるために、キーデータ自体のコピーは容易となることから、ユーザーが一度キーデータを入手した後は不正コピーが可能であり、不正コピー防止が不完全となるという不具合があった。そこで、各コンピュータがネットワークにて接続されている場合は、同じネットワーク内では同じキーデータを用いてインストールしたソフトウェアが同時に起動しないようにすると云ったプロテクトも採用されているが、個人ユーザーやネットワークに繋がっていないスタンドアロンで運用されているコンピュータへの不正コピーを防止することは出来なかった。本発明は、上記問題点を解決すべくなされたものであって、CD-ROM等の読み出し専用の記録媒体によるソフトウェアの提供であっても、ユーザーのコンピュータのみにインストール可能なキーデータを用いた不正コピー防止方法を提供することを目的とする。

## 【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】発明の詳細な説明

【補正方法】変更

【補正内容】

【発明の詳細な説明】

【0016】

【発明の効果】以上説明した如く本発明に係るソフトウェアの不正コピー防止方法は、CD-ROM等の読み出し専用の記録媒体によるソフトウェアの提供であっても、インストールを継続する為のキーデータを、コンピュータの固有情報にて暗号化し、ユーザーに提供するものであるから、固有情報の異なる他のコンピュータへの不正コピーを確実且つ容易に防止する上で著しい効果を奏する。

## 【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】図面の簡単な説明

【補正方法】変更

【補正内容】

【図面の簡単な説明】

【符号の説明】

ST1～ST10 ……ステップ1～ステップ10